

REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

The specification has been amended to include headings.

Amendments of a formal nature have been made to claims 15, 18, 21 and 24.

These amendments are not made for reasons relating to patentability.

Claims 21-26 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter.

Applicant respectfully submits that claims 21-26 fall within the statutory category of patentable subject matter under 35 U.S.C. Section 101 of a machine. Specifically, these claims define a "system" comprising the elements of a "file-type analyser" and "a start-up code searcher" or "an entry point code analyzer" which are defined as being operative to perform particular functions, and so are clearly directed to a computer system. As set forth in Annex II of the "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility," the Supreme Court has defined a machine as "a concrete thing, consisting of parts or of certain devices and combinations of devices." *Burr v. Duryee*, 68 U.S. (1 Wall) 531, 570 (1863). Applicant submits that claims 21-26 define such a machine, as being directed to a computer system. To further emphasize this, claims 21 and 24 have each been amended to refer to a "computer" system.

The office action contends that the claims are an example of "functional descriptive material." Applicant disagrees. The features of "a file-type analyser", "a start-up code searcher" and "an entry point code analyser" are operative to perform particular functions. Thus, the claims properly define elements of a machine, not descriptive material.

Consequently, withdrawal of the Section 101 rejection of claims 21-26 is respectfully requested.

Claims 15-26 were rejected under 35 U.S.C. Section 103(a) as allegedly being made "obvious" by Nachenberg (U.S. Patent No. 6,971,019) in view of Kephart et al. (U.S. Patent No. 5,675,711). Applicant respectfully traverses this rejection.

Claim 15 recites a scanning step of:

scanning the executable image, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type.

Nachenberg does not disclose such scanning and, consequently, Nachenberg also does not disclose the flagging step of claim 15 which occurs in response to a determination in the scanning.

Nachenberg discloses a number of techniques for scanning an executable image for certain data structures which are indicative of a virus. However, none of these techniques involves scanning for a data structure which is "start-up code ... generated by one of the compilers used to generate the determined file type."

The office action relies on column 9, lines 33-46 of Nachenberg as disclosing the claimed scanning. Applicant respectfully disagrees. This passage of Nachenberg relates to scanning of areas of the file "for virus strings" (see column 5, line 5). Such a "virus string" is not "start-up code...generated by one of the compilers used to generate the determined file type" as recited in claim 15. To the contrary, Nachenberg is referring to a conventional virus signature as disclosed at column 1, lines 12-22 which states "the simple virus can be easily detected by searching in files for a specific string of bytes (i.e. a 'signature') that has been extracted from the virus." Such a "virus string" is different from start-up code generated by a compiler. For example a "virus string" or signature is typically a piece of code which is unique to a single virus. In contrast, start-up code is code generated by a compiler and thus is present in any executable image compiled by the compiler concerned.

Although Nachenberg discloses at column 9, lines 41-42 that the scan may be performed at regions other than the entry point, the scanning step of claim 15 is different because the claim 15 scanning scans for different data than Nachenberg. In addition, the feature of the scanning being performed "with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types" is not disclosed in Nachenberg.

Claim 15 is not made obvious by Nachenberg and Kephart because these documents contain no disclosure relevant to the idea of using start-up code generated by a compiler as indicative of a virus. As discussed above, claim 15 involves "scanning the

executable image ... for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type." In response, the executable image may be flagged as suspicious. Thus the virus detection technique of claim 15 is based on the idea that if there is start-up code generated by one of the compilers used to generate the determined file type at a location other than said entry point, the executable image is suspicious. This is because such start-up code would normally be located at the entry point, so the presence of the start-up code at another location is indicative of a virus. The idea of using start-up code generated by compilers in this manner would not have been obvious from Nachenberg or Kephart et al.

The office action also refers to the disclosure on column 7, lines 10-21 of Nachenberg. This passage teaches (1) that a virus can modify the entry point and (2) that a virus can modify a JMP or CALL instruction. This information is used to determine where in the executable image to scan for a virus, as disclosed at column 9, lines 33-46 of Nachenberg. However, this does not teach or suggest the idea of scanning for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type. Consequently, the referenced portion of Nachenberg would not have made claim 15 obvious. Moreover, the claimed subject matter is not made obvious by any other portion of Nachenberg.

Applicant submits that Kephart et al. also fails to disclose or suggest the idea of scanning for start-up code at a location other than said entry point generated by one of the

compilers used to generate the determined file type. Consequently, Kephart et al. fails to remedy the deficiencies of Nachenberg.

Considering the comments in the office action regarding Kephart et al., the reference to Kephart et al. as disclosing "the layout to which the executable image conforms" is not understood, because "a database of known executable image layouts" is not an element of claim 15.

The office action references column 2, lines 1-15 of Kephart et al. Applicant submits that this passage does not disclose or suggest the idea of scanning for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type. To the contrary this passage is not relevant at all. Kephart et al. is generally concerned with a classifier which can distinguish between classes of data strings. Column 1 of Kephart et al. describes an application of such a classifier in virus detection. The passage on which the office action relies at column 2, lines 1-15 simply discloses another application of such a classifier, as is clear from the preceding sentence and the words "another example." This application of a classifier is to recognize a compiler for the purpose of reverse engineering of software. In other words, the passage goes no further than indicating that a classifier which can distinguish between classes of data strings may be used for identifying a compiler for the purpose of reverse engineering of software.

Thus, the passage of Kephart et al. on which the office action relies at column 2, lines 1-15 does not disclose anything about the start-up code generated by the compiler.

Thus the elements of claim 15 relating to "scanning the executable image ... for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type", and in response flagging the executable image as suspicious, are not obvious from Kephart et al., because Kephart et al. contains no suggestion of using start-up code generated by a compiler in this way.

Considering independent claim 18, Applicant submits that the reasoning in the office action is deficient because it does not set out where the elements of claim 18 are taught in Nachenberg and Klephart. The comments in the office action regarding claim 18 are set out in paragraph 4. However, all the comments relate to the elements of claim 15 as filed. Claim 18 recites different elements which are not referred to in paragraph 4 of the office action.

In particular, claim 18 recites the following elements which are not referred to in the Office Action:

determining, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, whether the executable image has at said entry point code similar to start-up code generated by one of the compilers used to generate the determined file type but with the beginning of this code having been changed; and

flagging the executable image as suspicious from the point of view of possibly containing a virus infection in response to determining that the executable image has said code at said entry point.

Furthermore, Applicant submits that these elements are not in fact taught in Nachenberg or Klephart et al. Essentially, this is for similar reasons to those presented above with respect to claim 15, namely that neither Nachenberg nor Kephart et al. contain

SHIPP, A.

Appl. No. 10/500,955

Response to Office Action dated October 19, 2007

any disclosure relevant to the idea of using start-up code generated by a compiler as indicative of a virus.

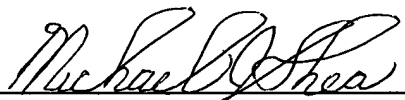
Claims 21 and 24 contain corresponding features to claims 15 and 18, respectively, and patentably distinguish over the applied references for similar reasons to those presented above with respect to claims 15 and 18.

The remaining claims patentably distinguish by virtue of their dependency from one of claims 15, 18, 21 and 24 and because of the other patentable features recited therein.

The pending claims patentably distinguish over the applied references and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Michael J. Shea
Reg. No. 34,725

MJS:mjs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100